円分関数体のゼータ多項式の可除性について (解析的整数論とその周辺)

AUTHOR(S):

塩見, 大輔

CITATION:

塩見, 大輔. 円分関数体のゼータ多項式の可除性について (解析的整数論とその周辺). 数理解析研究所講究録 2019, 2131: 113-120

ISSUE DATE:

2019-10

URL:

http://hdl.handle.net/2433/254772

円分関数体のゼータ多項式の可除性について

山形大学・理学部　塩見　大輔
Daisuke Shiomi
Faculty of Science, Yamagata University

素数 p と自然数 r に対して, 位数 $q = p^r$ の有限体 $\mathbb{F}_q$ を考える. また $K = \mathbb{F}_q(T)$, $\mathbb{A} = \mathbb{F}_q[T]$ とし, さらに $\mathbb{A}$ においてモニックなもの全体を $\mathbb{A}^+$ で表す. 自然数 n に対して,

$$(GB)_n = \begin{cases} \displaystyle\sum_{i=0}^{\infty} s_i(n) & n \not\equiv 0 \mod q-1 \text{ のとき}, \\ \displaystyle\sum_{i=0}^{\infty} -i s_i(n) & n \equiv 0 \mod q-1 \text{ のとき} \end{cases}$$

と置く. ただし,

$$s_i(n) = \sum_{\substack{a \in \mathbb{A}^+ \\ \deg a = i}} a^n.$$

多項式 $(GB)_n$ は Goss-Bernoulli 多項式と呼ばれ, 円分関数体の因子類群と密接な関係を持つ. Goss [3] は円分関数体の類数の p 可除性に関して Goss-Bernoulli 多項式による判定法を与えた (定理 3 を参照). これは円分体の類数に関するクンマーの判定法の関数体類似と見ることができる. またこの判定法の応用として, 類数が p 可除な円分関数体の無限族が構成できる (定理 4 を参照).

本稿では Goss-Bernoulli 多項式を一般化し, Goss の結果をゼータ多項式の観点から拡張することを考える. この応用として, 与えられた既約多項式に対して, それをゼータ多項式の既約成分に持つ円分関数体の無限族が構成できることを述べる.

1　円分関数体

ここでは, 円分関数体について簡単に復習しておく. 詳しくは文献 [4], [5], [6] を参照のこと.

体 K^{ac} を K の代数閉包とし, $\mathbb{F}_q$ 上の線形写像 φ, μ を次で定める.

$$\varphi : K^{ac} \to K^{ac} \quad (x \mapsto x^q),$$
$$\mu : K^{ac} \to K^{ac} \quad (x \mapsto Tx).$$

これらを用いて K^{ac} に次で $\mathbb{A}$ 加群の構造を入れる.

$$N * x = N(\varphi + \mu)(x) \quad (N \in \mathbb{A},\ x \in K^{ac}).$$

この加群を Carlitz 加群と呼ぶ. Carlitz 加群の N 等分点全体

$$\Lambda_N = \{x \in K^{ac} \mid N * x = 0\}$$

を考える. このとき, $K_N = K(\Lambda_N)$ を N 円分関数体と呼ぶ.

例 1 $N = T$ のとき, $T * x = x^q + Tx$ なので

$$\Lambda_T = \{x \in K^{ac} \mid x^q + Tx = 0\}.$$

従って, $K_T = K(\Lambda_T) = K(\sqrt[q-1]{-T}\,)$.

上の Λ_N は $\mathbb{A}$ 加群として巡回的である. つまり, ある $\lambda_N \in \Lambda_N$ を用いて

$$\Lambda_N = \mathbb{A} * \lambda_N$$

と表せる.

定理 1 (cf. [5]) K_N/K は *geometric* なガロア拡大である. またガロア群 $G(K_N/K)$ に関して以下の同型が成り立つ.

$$(\mathbb{A}/N\mathbb{A})^\times \to G(K_N/K)\ \ (A \mod N \mapsto \sigma_{A \mod N}). \tag{1}$$

ただし, 準同型 $\sigma_{A \mod N}$ は $\sigma_{A \mod N}(\lambda_N) = A * \lambda_N$ で定まるものとする.

次に, K の素点 ∞ で対応する付値が $\mathrm{ord}_\infty(T) < 0$ を満たすものを無限素点と呼ぶことにする (そのような素点は K においてただ一つだけ存在する). K_∞ を K の無限素点 ∞ による完備化とする. また

$$K_N^+ = K_N \cap K_\infty$$

とし, これを K_N の最大実部分体と呼ぶ. ガロア群 $G(K_N/K)$ と $(\mathbb{A}/N\mathbb{A})^\times$ を同一視したとき, K_N^+ は $\mathbb{F}_q^\times$ に対応する中間体である. 特に

$$[K_N : K_N^+] = q - 1 \tag{2}$$

が分かる. 従って $\deg N = 1$ のとき $K = K_N^+$ であり, $q = 2$ のときは $K_N^+ = K_N$ が成り立つ.

次に K_N, K_N^+ の類数 (=次数 0 の因子類群の位数) をそれぞれ h_N, h_N^+ で表す. このとき, h_N^+ は h_N を割ることが知られている (文献 [6] の 14 章を参照). そこで,

$$h_N^- = \frac{h_N}{h_N^+}$$

とし, これを K_N の相対類数と呼ぶ. $q = 2$ のときは $h_N^- = 1$ に注意する.

2 Gossの結果

この節では, 円分関数体の類数に関するGossの結果を紹介する. 詳細は論文 [2], [3] を参照のこと.

自然数 n に対して q 進展開が

$$n = a_0 + a_1 q + \cdots + a_{d-1} q^{d-1} \ (0 \le a_i \le q-1)$$

で与えられるとき, 整数 $l(n)$ を次で定める.

$$l(n) = a_0 + a_1 + \cdots + a_{d-1}.$$

また, 整数 e_i $(1 \le i \le l(n))$ を次を満たすように取る.

$$n = \sum_{i=1}^{l(n)} q^{e_i} \quad (0 \le e_i \le e_{i+1}, \ \ e_i < e_{i+q-1}).$$

このとき,

$$\rho(n) = \begin{cases} -\infty & l(n) < q-1 \text{ のとき}, \\ n - \displaystyle\sum_{i=1}^{q-1} q^{e_i} & \text{それ以外のとき} \end{cases}$$

と置く. ただし, $\rho(-\infty) = -\infty$ とする. さらに,

$$\rho^{(0)}(n) = n, \quad \rho^{(i)} = \rho^{(i-1)} \circ \rho \ \ (i \ge 1)$$

により帰納的に $\rho^{(i)}(n)$ を定める.

定理 2 (cf. [2]) 整数 $i \ge 1$ に対して,

$$\deg_T(s_i(n)) \le \rho^{(1)}(n) + \rho^{(2)}(n) + \cdots + \rho^{(i)}(n). \tag{3}$$

特に $l(n)/(q-1) < i$ ならば, $s_i(n) = 0$ である.

定理 2 より, $(GB)_n \in \mathbb{A}$ が分かる. Goss [3] は $(GB)_n$ を用いて Kummer の判定法の関数体類似に相当する次の結果を与えた.

定理 3 (cf. [3]) d 次既約 $N \in \mathbb{A}^+$ に対して次が成立する.

(1) $p \mid h_N^- \iff$ 整数 $1 \le n \le q^d - 2$ $(n \not\equiv 0 \mod q-1)$ で, $N \mid (GB)_n$ を満たすものが存在する.

(2) $p \mid h_N^+ \iff$ 整数 $1 \le n \le q^d - 2$ $(n \equiv 0 \mod q-1)$ で, $N \mid (GB)_n$ を満たすものが存在する.

d 次既約 $N \in \mathbb{A}^+$ に対して, $n_1 \equiv n_2 \mod q^d - 1$ ならば,

$$(GB)_{n_1} \equiv (GB)_{n_2} \mod N \tag{4}$$

が成り立つことが分かる. この合同性と定理 3 を用いることで次が導かれる.

定理 4 (cf. [1], [3])

(1) $q \neq 2$ のとき, $p \mid h_N^-$ を満たす既約 $N \in \mathbb{A}^+$ が無限に存在する.

(2) $p \mid h_N^+$ を満たす既約 $N \in \mathbb{A}^+$ が無限に存在する.

補足 1 定理 4 は, まず Goss [3] により $q = p$ の条件下でマイナスパートの場合が証明され, その後, Feng [1] によりプラス, マイナス, 両方の場合に関して一般的な証明がなされた.

3 ゼータ関数

ここでは, 大域関数体のゼータ多項式について簡単に復習する. 詳細は文献 [6], [7] を参照のこと.

$\mathbb{F}_q$ 上の大域関数体 L に対して, そのゼータ関数を

$$\zeta(s, L) = \prod_{P:\text{prime}} \left(1 - \frac{1}{N(P)^s}\right)^{-1}$$

で定める. ここで P は L の素点全体を渡り, $N(P)$ は P の剰余体の位数とする. 上のオイラー積は $\mathrm{Re}(s) > 1$ で収束する.

定理 5 種数 g_L の $\mathbb{F}_q$ 上の大域関数体 L を考える. このとき, 次を満たす $2g_L$ 次の整数係数多項式 $Z_L(X)$ が存在する.

$$\zeta(s, L) = \frac{Z_L(q^{-s})}{(1 - q^{-s})(1 - q^{1-s})}.$$

さらに,

$$Z_L(0) = 1, \quad Z_L(1) = h_L$$

が成り立つ. ただし, h_L は L の類数とする. 上の多項式 $Z_L(X)$ を L のゼータ多項式と呼ぶ.

次に円分関数体の場合を考察する. K_N, K_N^+ のゼータ多項式をそれぞれ $Z_N(X)$, $Z_N^{(+)}(X)$ で表す. このとき, $Z_N^{(+)}(X)$ は $Z_N(X)$ を割ることが分かる (cf. [7]). そこで

$$Z_N^{(-)}(X) = \frac{Z_N(X)}{Z_N^{(+)}(X)}$$

と置く. また, g_N, g_N^+ をそれぞれ K_N, K_N^+ の種数とし, さらに

$$g_N^- = g_N - g_N^+$$

とする. このとき, 定理 5 から

$$\deg Z_N^{(+)}(X) = 2g_N^+, \quad \deg Z_N^{(-)}(X) = 2g_N^-$$

であり, また

$$Z_N^{(+)}(1) = h_N^+, \quad Z_N^{(-)}(1) = h_N^-$$

であることも分かる.

例 2 $q = p = 2$, $N = T^3 + T + 1$ の場合を考える. このとき,

$$Z_N^{(+)}(X) = 8X^6 + 16X^5 + 18X^4 + 15X^3 + 9X^2 + 4X + 1$$

となる. 従って, $g_N^+ = 3$, $h_N^+ = Z_N^{(+)}(1) = 71$ を得る.

例 3 $q = p = 3$, $N = T^2 + 1$ の場合を考える. このとき,

$$Z_N^{(-)}(X) = 9X^4 - 2X^2 + 1$$

となる. 従って, $g_N^- = 1$, $h_N^- = Z_N^{(-)}(1) = 8$ を得る.

4 主結果

ここでは, Goss-Bernoulli 多項式の一般化について考察し, さらに定理 4, 定理 5 がゼータ多項式の観点から拡張できることを述べる. 本節の内容の詳細は文献 [8] を参照のこと.

まず,

$$B_n(X) = \begin{cases} \displaystyle\sum_{i=0}^{\infty} s_i(n) X^i & n \not\equiv 0 \mod q-1 \text{ のとき}, \\ \displaystyle\sum_{i=0}^{\infty} \left(\sum_{j=0}^{i} s_j(n) \right) X^i & n \equiv 0 \mod q-1 \text{ のとき} \end{cases}$$

と置く. 定理 2 より, $B_n(X) \in \mathbb{A}[X]$ となる. $\mathbb{F}_q^{ac}$ を $\mathbb{F}_q$ の代数閉包とし, $\alpha \in \mathbb{F}_q^{ac}$ に対して, $\mathbb{F}_\alpha = \mathbb{F}_q(\alpha)$ とする. このとき,

$$(GB)_{\alpha,n} = N_{\mathbb{F}_\alpha(T)/\mathbb{F}_q(T)}(B_n(\alpha)) \in \mathbb{A} \quad (n \geq 1)$$

と置く. ただし, $N_{\mathbb{F}_\alpha(T)/\mathbb{F}_q(T)}$ は $\mathbb{F}_\alpha(T)$ から $\mathbb{F}_q(T)$ へのノルムである. この多項式 $(GB)_{\alpha,n}$ を α に付随する Goss-Bernoulli 多項式と呼ぶ. 特に $\alpha = 1$ のとき, $(GB)_{1,n} = (GB)_n$ である. 次に,

$$\bar{Z}_N^{(\pm)}(X) = Z_N^{(\pm)}(X) \mod p \in \mathbb{F}_p[X]$$

と置く.

主結果 1 (cf. [8]) $\alpha \in \bar{\mathbb{F}}_q$ の $\mathbb{F}_p$ 上の最小多項式を $f(X)$ と置く. d 次既約 $N \in \mathbb{A}^+$ に対して次が成り立つ.

(1) $f(X) \mid \bar{Z}_N^{(-)}(X) \iff$ 整数 $1 \leq n \leq q^d - 2$ $(n \not\equiv 0 \mod q-1)$ で $N \mid (GB)_{\alpha,n}$ を満たすものが存在する.

(2) $f(X) \mid \bar{Z}_N^{(-)}(X) \iff$ 整数 $1 \leq n \leq q^d - 2$ $(n \not\equiv 0 \mod q-1)$ で $N \mid (GB)_{\alpha,n}$ を満たすものが存在する.

$\alpha = 1$ の場合を考える. このとき, $f(X) = X - 1$ であり, $Z_N^{(-)}(1) = h_N^-$, $Z_N^{(+)}(1) = h_N^+$ に注意すれば,

$$p \mid h_m^- \iff f(X) \mid \bar{Z}_m^{(-)}(X), \tag{5}$$

$$p \mid h_m^+ \iff f(X) \mid \bar{Z}_m^{(+)}(X) \tag{6}$$

が分かる. また $(GB)_{\alpha,1} = GB_n$ であったので, 主結果 1 から定理 3 が導かれる.

例 4 $q = p = 2$ とし, α を $\mathbb{F}_2$ 上の既約多項式 $f(X) = X^3 + X^2 + 1$ の根とする. このとき, $(GB)_{\alpha,n}$ $(1 \leq n \leq 6 = 2^3 - 2)$ は次のようになる.

$$(GB)_{\alpha,n} = 1 + s_1(n) + s_1(n)s_2(n) + s_2(n)^2 + s_1(n)^3 + s_1(n)s_2(n)^2 + s_2(n)^3.$$

ただし,

$$\begin{aligned} s_1(n) &= T^n + (1+T)^n, \\ s_2(n) &= (T^2)^n + (1+T^2)^n + (T+T^2)^n + (1+T+T^2)^n. \end{aligned}$$

$\mathbb{F}_2[T]$ 上での $(GB)_{\alpha,n}$ の既約分解は次で与えられる.

$$\begin{aligned} (GB)_{\alpha,1} &= 1, \\ (GB)_{\alpha,2} &= 1, \\ (GB)_{\alpha,3} &= (1+T+T^3)(1+T^2+T^3), \\ (GB)_{\alpha,4} &= 1, \\ (GB)_{\alpha,5} &= (1+T+T^3)(1+T^2+T^3)(1+T^2+T^3+T^5+T^6), \\ (GB)_{\alpha,6} &= (1+T+T^3)^2(1+T^2+T^3)^2. \end{aligned}$$

例えば, $N = T^3 + T + 1$ の場合を考えると,

$$N \mid (GB)_{\alpha,3}, \qquad N \mid (GB)_{\alpha,5}, \quad N \mid (GB)_{\alpha,6}.$$

従って, 主結果 1 より $f(X) \mid \bar{Z}_N^{(+)}(X)$ である. 実際, 例 2 より,

$$Z_N^{(+)}(X) \equiv X^3 + X^2 + 1 \mod 2$$

となっていることが分かる.

例 5 $q = p = 3$ とし, $\mathbb{F}_3$ 上の既約多項式

$$f(X) = X^2 + 2X + 2 = (X - \alpha)(X - \beta)$$

を考える. $1 \leq n \leq 3^2 - 2 = 7$ $(n \not\equiv 0 \bmod 2)$ のとき,

$$B_n(X) = 1 + s_1(n)X.$$

従って,

$$(GB)_{\alpha,n} = (1 + s_1(n)\alpha)(1 + s_1(n)\beta) = 1 + 2s_1(n) + s_1(n)^2.$$

ただし,

$$s_1(n) = T^n + (1 + T)^n + (2 + T)^n.$$

このとき, $(GB)_{\alpha,n}$ の既約分解は次で与えられる.

$$\begin{aligned}
(GB)_{\alpha,1} &= 1, \\
(GB)_{\alpha,3} &= 1, \\
(GB)_{\alpha,5} &= 2(2 + 2T + T^2 + T^3 + T^4 + T^6), \\
(GB)_{\alpha,7} &= 2(2 + T + T^2 + 2T^3 + T^4 + T^6).
\end{aligned}$$

例えば, $N = T^2 + 1$ の場合を考えると, 主結果 1 より $f(X) \nmid \bar{Z}_N^{(-)}(X)$ である. 実際, 例 3 より,

$$Z_N^{(-)}(X) \equiv X^2 + 1 \mod 3$$

であり, $\bar{Z}_N^{(-)}(X)$ は $f(X)$ を既約因子に持たない.

等式 (4) で見た $(GB)_n$ の合同性は $(GB)_{\alpha,n}$ に一般化することができる. d 次既約 $N \in \mathbb{A}^+$ に対して, $n_1 \equiv n_2 \mod q^d - 1$ のとき,

$$(GB)_{\alpha,n_1} \equiv (GB)_{\alpha,n_2} \mod N \tag{7}$$

が成り立つ. この合同性と主結果 1 を用いることで次の結果が導かれる.

主結果 2 (cf. [8])

(1) $q \neq 2$ のとき, $f(X) \mid \bar{Z}_N^{(-)}(X)$ を満たす既約 $N \in \mathbb{A}^+$ が無限に存在する.

(2) $f(X) \mid \bar{Z}_N^{(+)}(X)$ を満たす既約 $N \in \mathbb{A}^+$ が無限に存在する.

$f(X) = X - 1$ の場合を考える. このとき, 等式 (5), (6) により, 主結果 2 から定理 4 が従うことが分かる.

参考文献

[1] K. Feng, A note on irregular prime polynomials in cyclotomic function field theory, J. Number Theory **22** (1986), 240–245.

[2] E. U. Gekeler, On power sums of polynomials over finite fields, J. Number Theory **30** (1988), 11–26.

[3] D. Goss, Kummer and Herbrand criterion in the theory of function fields, Duke Math. J. **49** (1982), 377–384.

[4] D. Goss, Basic Structures of Function field Arithmetic, Springer-Verlag, Berlin, 1998.

[5] D. R. Hayes, Explicit class field theory for rational function fields, Trans. Amer. Math. Soc. **189** (1974), 77–91.

[6] M. Rosen, Number Theory in Function Fields, Springer-Verlag, Berlin, 2002.

[7] D. Shiomi, A determinant formula for relative congruence zeta functions for cyclotomic function fields, J. Aust. Math. Soc. **89** (2010), 133-144.

[8] D. Shiomi, *The divisibility of zeta functions of cyclotomic function fields*, arXiv:1808.06782.